Oracle® Hardware Management Pack セキュリティーガイド

Part No: E39910-02
2015 年 10 月

Part No: E39910-02

Copyright © 2014, 2015, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、Oracle Corporationおよびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはオラクル およびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`) か、聴覚に障害のあるお客様は (`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`)を参照してください。

目次

概要 7
製品の概要 7
このセキュリティーガイドについて 8
基本的なセキュリティー原則 8
Oracle Hardware Management Pack のセキュリティーに関するサマリー 9

Oracle Hardware Management Pack インストール前 11
Oracle Hardware Management Pack のコンポーネント 11
エージェントに基づいた SNMP Plugin セキュリティー設定 12
SNMP エージェントの SNMP プロトコルバージョンの選択 12

Oracle Hardware Management Pack のインストール 13
Oracle Hardware Management Pack インストーラの実行 13
ホストと ILOM の相互接続を有効にする選択 13
ファイルでの資格情報の保存の選択 14

Oracle Hardware Management Pack インストール後 17
Oracle Hardware Management Pack のアンインストール 17

概要

このセクションでは、セキュリティーガイド情報を含む Oracle Hardware Management Pack 製品の概要を示し、アプリケーションセキュリティーの一般的な原則について説明します。

次のトピックで構成されています。

- 7 ページの「製品の概要」
- 8 ページの「このセキュリティーガイドについて」
- 8 ページの「基本的なセキュリティー原則」
- 9 ページの「Oracle Hardware Management Pack のセキュリティーに関するサマリー」

製品の概要

Oracle Hardware Management Pack は、多くの x86 ベースのサーバーと一部の SPARC ベースのサーバーで利用できます。Oracle Hardware Management Pack には、サーバーを管理するために 2 つのコンポーネント (SNMP モニタリングエージェントと、クロスオペレーティングシステムコマンド行インタフェースツール (CLI ツール) のファミリ) が用意されています。

Hardware Management Agent SNMP Plugins を使用すると、SNMP を使用してデータセンター内の Oracle サーバーおよびサーバーモジュールをモニターでき、2 つの管理ポイント (ホストと Oracle ILOM) に接続する必要がないという利点が得られます。この機能により、単一の IP アドレス (ホストの IP) を使用して、複数のサーバーおよびサーバーモジュールをモニターできます。

Hardware Management Agent SNMP Plugins は、Oracle サーバーのホストオペレーティングシステム上で動作します。SNMP Plugins では、サービスプロセッサとの通信に Oracle Hardware Storage Access Libraries が使用されます。サーバーの現在の状態に関する情報が Hardware Management Agent によって自動的に取得されます。Hardware Management Agent の詳細については、『*Oracle Server Management Agents* ユーザーズガイド』を参照してください。

Oracle Server CLI ツールを使用して、Oracle サーバーを構成できます。CLI ツールは、Oracle Solaris、Oracle Linux、Oracle VM、その他の Linux バリアント、および

Windows オペレーティングシステムで動作します。ツールのリストについては、『*Oracle Server CLI* ツールユーザーズガイド』を参照してください。

機能と使用法の詳細については、Oracle Hardware Management Pack for Oracle Solaris のドキュメントを参照してください。

- Oracle Hardware Management Pack のドキュメントライブラリ: `http://www.oracle.com/goto/ohmp/docs`
- 一般的な Oracle ILOM の情報については、`http://www.oracle.com/goto/ilom/docs` を参照してください

このセキュリティーガイドについて

このドキュメントでは、Oracle Hardware Management Pack の一般的なセキュリティーガイドラインについて説明します。このガイドは、ネットワークスイッチやネットワークインタフェースカードなどのほかの Oracle ハードウェア製品と一緒にこのソフトウェアを使用するときに、セキュリティーを確保するのを支援することを意図しています。

次のトピックで構成されています。

- 11 ページの「Oracle Hardware Management Pack インストール前」
- 13 ページの「Oracle Hardware Management Pack のインストール」
- 17 ページの「Oracle Hardware Management Pack インストール後」

基本的なセキュリティー原則

基本的なセキュリティー原則として、アクセス、認証、承認、およびアカウンティングの 4 つがあります。

- アクセス

  物理的およびソフトウェア制御を使用して、ハードウェアやデータを侵入から保護します。

  - ハードウェアの場合、アクセス制限は通常、物理的なアクセス制限を意味します。
  - ソフトウェアの場合は通常、アクセス制限は物理的および仮想的な手段の両方を意味します。
  - ファームウェアは、Oracle 更新プロセス以外では変更できません。
- 認証

プラットフォームオペレーティングシステムにパスワードシステムなどのあらゆる認証機能を設定することで、ユーザーが本人であることを確認します。

認証では、バッジやパスワードなどの手段を通じてさまざまなレベルのセキュリティーを提供します。たとえば、担当者がコンピュータ室に入室する際は、従業員バッジを正しく使用してもらうようにします。

- 承認

  承認では、会社の担当者に対して、トレーニングを受けて使用を許可されたハードウェアやソフトウェアのみの操作を許可します。

  たとえば、システムの読み取り/書き込み/実行アクセス権を設定することで、コマンド、ディスク領域、デバイス、およびアプリケーションへのユーザーアクセスを制御します。

- アカウンティング

  顧客の IT 担当者は、Oracle のソフトウェアおよびハードウェア機能を使用して、ログインアクティビティーをモニターしたりハードウェアインベントリを保守したりします。

  - システムログを使用して、ユーザーログインをモニターします。特に、システム管理者アカウントとサービスアカウントは強力なコマンドにアクセスできるため、これらのアカウントはシステムログで追跡します。
  - ログファイルが適当なサイズを超えたときは、顧客の会社方針に従って定期的に回収します。ログは一般的に長期間保持されるため、保持する方法が重要となります。
  - インベントリ目的でシステム資産を追跡する場合は、コンポーネントシリアル番号を使用します。すべてのカード、モジュール、およびマザーボードには、Oracle パーツ番号が電子的に記録されています。

Oracle Hardware Management Pack のセキュリティーに関するサマリー

すべてのシステム管理ツールを構成するときに留意する必要のある、重要なセキュリティー項目は次のとおりです。

- システム管理製品を使用して、ブート可能なルート環境を構築できます。

  ブート可能なルート環境では、Oracle ILOM、Oracle System Assistant、およびハードディスクへのアクセス権が与えられます。

- システム管理製品には、実行するのに管理者およびルート特権を必要とする強力なツールが含まれています。

  このレベルのアクセス権で、ハードウェア構成を変更したり、データを消去したりできます。

Oracle Hardware Management Pack インストール前

初期インストールおよび設定の間、Oracle ソフトウェアセキュリティー機能を使用して、ハードウェアを制御し、システム資産を追跡します。

次のトピックで構成されています。

- 11 ページの「Oracle Hardware Management Pack のコンポーネント」
- 12 ページの「エージェントに基づいた SNMP Plugin セキュリティー設定」
- 12 ページの「SNMP エージェントの SNMP プロトコルバージョンの選択」

Oracle Hardware Management Pack のコンポーネント

Oracle Hardware Management Pack には、RAID、BIOS、Oracle ILOM を構成し、ファームウェアを更新するための、一連のハードウェア管理コマンド行ツールが含まれています。モニター用の SNMP Plugin も含まれています。Oracle Hardware Management Pack には、内部チャネルを介して Oracle ILOM と通信し、サーバーに関するインベントリおよび健全性情報を共有するデーモンまたはサービスも含まれます。

これらのツールとプラグインはホストオペレーティングシステムにインストールされているので、ホストから直接システム管理タスクを実行できます。Oracle Hardware Management Pack には、Oracle サーバーの管理に役立つ機能が用意されていますが、これは完全にオプションです。

Oracle Hardware Management Pack 機能の詳細については、次のドキュメントライブラリを参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)
- Oracle ILOM のドキュメントライブラリ (`http://www.oracle.com/goto/ilom/docs`)

エージェントに基づいた SNMP Plugin セキュリティー設定

Oracle Hardware Management Pack には、ホストオペレーティングシステムのネイティブ SNMP エージェントを拡張して追加の Oracle MIB 機能を提供する SNMP Plugin モジュールが含まれています。Oracle Hardware Management Pack 自体には SNMP エージェントが含まれていないことに留意することが特に重要です。Linux の場合、モジュールは net-snmp エージェント (あらかじめインストールされている必要がある) に追加されます。Solaris の場合、モジュールは Solaris Management Agent に追加されます。Windows の場合、このプラグインはネイティブ SNMP サービスを拡張します。

同様に、Oracle Hardware Management Pack SNMP Plugin の SNMP に関連するセキュリティー設定は、プラグインによってではなく、ネイティブ SNMP エージェントまたはサービスの設定によって決まります。SNMP をセキュアに構成する方法については、net-snmp または Windows SNMP サービスのドキュメントを参照してください。次のリンクにある『*Oracle Server Management Agents* ユーザーズガイド』の手順も参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)

SNMP エージェントの SNMP プロトコルバージョンの選択

SNMP は、システムをモニターまたは管理するために使用される標準プロトコルです。SNMPv1/v2c は暗号化を備えておらず、認証の一形態としてコミュニティー文字列を使用します。コミュニティー文字列は平文のままネットワーク経由で送信され、個々のユーザー専用ではなく、通常は個人のグループ全体で共有されます。これに対し、SNMPv3 では暗号化を使用してセキュアチャネルを提供し、個別のユーザー名とパスワードを使用します。SNMPv3 のユーザーパスワードは、管理ステーション上にセキュアに格納できるようにローカライズされます。

ネイティブ SNMP エージェントでサポートされている場合は、SNMPv3 を使用することをお勧めします。SNMPv3 を構成する方法については、net-snmp (Oracle Solaris および Linux) または Windows SNMP サービスのドキュメントを参照してください。

Oracle Hardware Management Pack のインストール

次のトピックで構成されています。

- 13 ページの「Oracle Hardware Management Pack インストーラの実行」
- 13 ページの「ホストと ILOM の相互接続を有効にする選択」
- 14 ページの「ファイルでの資格情報の保存の選択」

Oracle Hardware Management Pack インストーラの実行

Oracle Hardware Management Pack は、RPM など、オペレーティングシステムのネイティブインストールツールを使用してインストールできる、一連のネイティブインストールパッケージから構成されます。さらに、ウィザードベースインストーラを使用することで、簡単にインストールできます。インストーラは、ネイティブのパッケージの追加以外にも、Oracle Hardware Management Pack を使用できるように構成するときにも役立ちます。

Oracle Hardware Management Pack インストーラは、ネイティブパッケージをインストールする必要があるので、ルートまたは管理者として実行する必要があります。詳細については、次のリンクにある『*Oracle Hardware Management Pack* インストールガイド』を参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)

ホストと ILOM の相互接続を有効にする選択

KCS インタフェースに替わる高速代替手段として、ホストオペレーティングシステム上のクライアントは、内蔵の高速インターコネクトを介して Oracle ILOM と通信できます。Oracle Hardware Management Pack では、この機能は「ホストと ILOM の相互接続」と呼ばれます。Oracle ILOM インタフェースでは、この機能は「ローカルホスト相互接続」と呼ばれます。このインターコネクトは、内蔵の Ethernet-over-USB 接続によって実装されており、IP スタックを実行します。Oracle ILOM およびホストには、

このチャネルで通信するためのルーティング不可能な内部 IP アドレスが与えられています。

ホストと ILOM の相互接続 (ローカルホスト相互接続) を介して Oracle ILOM に接続するには認証が必要になりますが、これはちょうど、接続がネットワーク経由で Oracle ILOM 管理ポートに入ってくる場合と同じです。管理ネットワーク上で公開されているサービスまたはプロトコルはすべて、ホストと ILOM の相互接続を介してホストから利用できます。たとえば、ホスト上の Web ブラウザを使用して Oracle ILOM Web インタフェースにアクセスしたり、Secure Shell クライアントを使用して Oracle ILOM CLI に接続したりできます。どのようなケースでも、ホストと ILOM の相互接続を使用するには、有効なユーザー名とパスワードを入力する必要があります。

Oracle Hardware Management Pack インストーラには、ホストと ILOM の相互接続を有効にするオプションが用意されています。ネットワーク手順で RFC 3927 と、リンクローカル IPv4 アドレスの割り当て機能をサポートしている場合にかぎり、ホストと ILOM の相互接続を有効にすることをお勧めします。また、オペレーティングシステムがブリッジまたはルーターとして機能していないことを慎重に確認してください。これにより、ホストと Oracle ILOM との間の管理トラフィックがプライベートのままであることが確実になります。詳細については、次のリンクにある『*Oracle Hardware Management Pack* インストールガイド』を参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)

ファイルでの資格情報の保存の選択

Oracle Hardware Management Pack 2.3.3 以降では、この機能が無効になっています。

Oracle Hardware Management Pack for Oracle Solaris に含まれている `ilomconfig` ツールと `fwupdate` ツールは、高速なホストと ILOM の相互接続を使用して Oracle ILOM に接続できます。ホストと ILOM の相互接続では認証が必要であるため、これらのツールを呼び出すたびに、Oracle ILOM で認証を受ける必要があります。便利な方法として、資格情報をファイルにキャッシュすることで、ツールは自動的にそれらを使用できます。これにより、Oracle Hardware Management Pack ツールを使用するスクリプトに平文パスワードを埋め込む必要がなくなります。

`ilomconfig` ツールを使用すると、ルートで読み取り専用の暗号化ファイルにユーザー名とパスワードを格納できます。`ilomconfig` または `fwupdate` を使用して Oracle ILOM にアクセスするときにこのファイルが検出された場合、キャッシュされた資格情報が使用されます。または、ツールを呼び出すごとに、コマンド行でユーザー名とパスワードを指定することもできます。

使用される暗号化アルゴリズムはシステムごとに異なります。ただし鍵が検出された場合は、ファイルを復号することで、ユーザー名とパスワードを暴露できます。危殆

化したパスワードをほかの Oracle ILOM システムで使用できないように、それぞれの Oracle ILOM で一意のパスワードを作成することをお勧めします。

資格情報をファイルに保存する方法については、次のリンクにある『*Oracle CLI Tools for Oracle Solaris* ユーザーズガイド』を参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)

Oracle Hardware Management Pack インストール後

次のトピックで構成されています。

- 17 ページの「Oracle Hardware Management Pack のアンインストール」

Oracle Hardware Management Pack のアンインストール

Oracle Hardware Management Pack パッケージは、RPM などのネイティブパッケージツールを使用するか、Oracle Hardware Management Pack に付属のウィザードベースアンインストーラを使用することで、アンインストールできます。ネイティブパッケージ方式を使用してパッケージを削除するときに、ホストと ILOM の相互接続を使用した Oracle ILOM へのアクセスが容易になるように、Oracle Hardware Management Pack を使用して事前にホスト資格情報をキャッシュファイルに保存した場合、そのファイルは削除されません。このようなケースでこのファイルを削除するには、Oracle Hardware Management Pack パッケージをアンインストールする前に、`ilomconfig delete credential` コマンドを実行してください。

ウィザードベースアンインストーラでは資格情報ファイルが削除されます。したがって、Oracle Hardware Management Pack のアンインストールには、ウィザードベースインストーラを使用することをお勧めします。詳細については、次のリンクにある『*Oracle Hardware Management Pack* インストールガイド』を参照してください。

- Oracle Hardware Management Pack ドキュメントライブラリ (`http://www.oracle.com/goto/ohmp/docs`)